US 20140101454A1

(19) **United States**

(12) **Patent Application Publication**

Thom et al.

(10) **Pub. No.: US 2014/0101454 A1**

(43) **Pub. Date: Apr. 10, 2014**

(54) SECURE CREDENTIAL UNLOCK USING TRUSTED EXECUTION ENVIRONMENTS

(71) Applicant: **Microsoft Corporation**, Redmond, WA (US)

(72) Inventors: **Stefan Thom**, Snohomish, WA (US); **Robert K. Spiger**, Seattle, WA (US); **Magnus NystrÖm**, Sammamish, WA (US); **Himanshu Soni**, Redmond, WA (US); **Marc R. Barbour**, Woodinville, WA (US); **Nick Voicu**, Bellevue, WA (US); **Xintong Zhou**, Bellevue, WA (US); **Kirk Shoop**, Seattle, WA (US)

(73) Assignee: **Microsoft Corporation**, Redmond, WA (US)

(21) Appl. No.: **14/105,070**

(22) Filed: **Dec. 12, 2013**

Related U.S. Application Data

(63) Continuation of application No. 13/176,735, filed on Jul. 5, 2011, now Pat. No. 8,612,766.

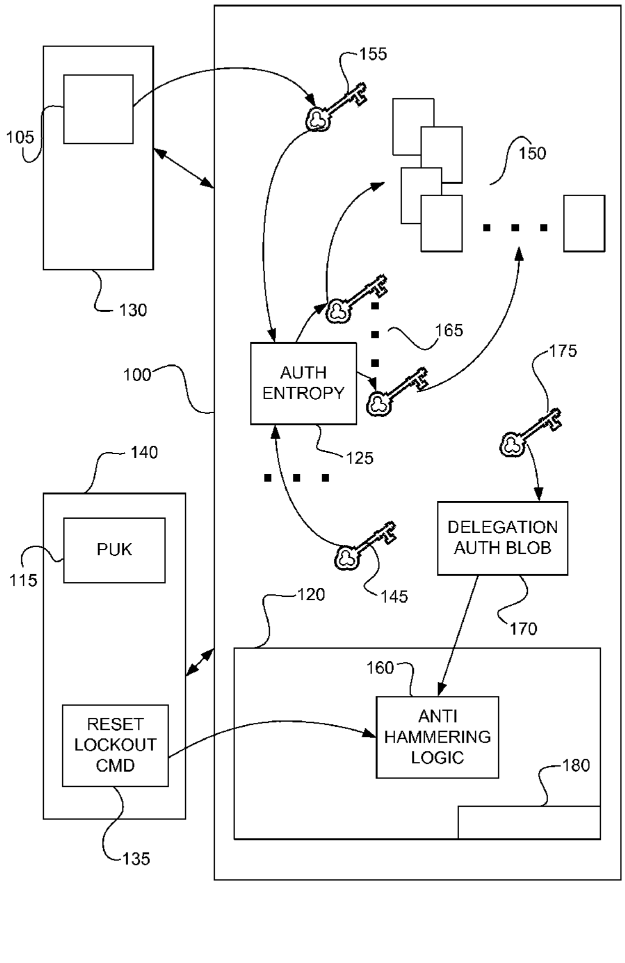
Publication Classification

(51) **Int. Cl.**
G06F 21/30 (2006.01)

(52) **U.S. Cl.**
CPC *G06F 21/30* (2013.01)
USPC **713/182**

(57) ABSTRACT

Computing devices utilizing trusted execution environments as virtual smart cards are designed to support expected credential recovery operations when a user credential, personal identification number (PIN), password, etc. has been forgotten or is unknown. A computing device generates a cryptographic key that is protected with a PIN unlock key (PUK) provided by an administrative entity. If the user PIN cannot be input to the computing device the PUK can be input to unlock the locked cryptographic key and thereby provide access to protected data. A computing device can also, or alternatively, generate a group of challenges and formulate responses thereto. The formulated responses are each used to secure a computing device cryptographic key. If the user PIN cannot be input to the computing device an entity may request a challenge. The computing device issues a challenge from the set of generated challenges. Upon receiving a valid response back, the computing device can unlock the secured computing device cryptographic key associated with the issued challenge and subsequently provide access to protected data.


155
105
150
130
165
175
100
AUTH ENTROPY
125
140
115
PUK
145
DELEGATION AUTH BLOB
120
170
160
ANTI HAMMERING LOGIC
RESET LOCKOUT CMD
180
135